The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/10/2013

SUBJECT:

Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution (MS13-099)

OVERVIEW:

A remote code execution vulnerability exists in Microsoft Scripting Runtime Object Library. The Microsoft Scripting Runtime Object Library contains objects that are useful for writing scripts. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows 7
- Windows Server 2008
- Windows Server 2012
- Windows 8 & 8.1
- Windows RT & RT 8.1

RISK: Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

This remote code execution vulnerability exists due to the way Microsoft Scripting Runtime Object Library handles objects in memory. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply the appropriate patch provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/MS13-099

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5056